資料2

スマートフォンにおける公的個人認証サービスの利活用環境実現に向けた調査研究結果

中間成果報告

2021年11月24日
株式会社NTTデータ

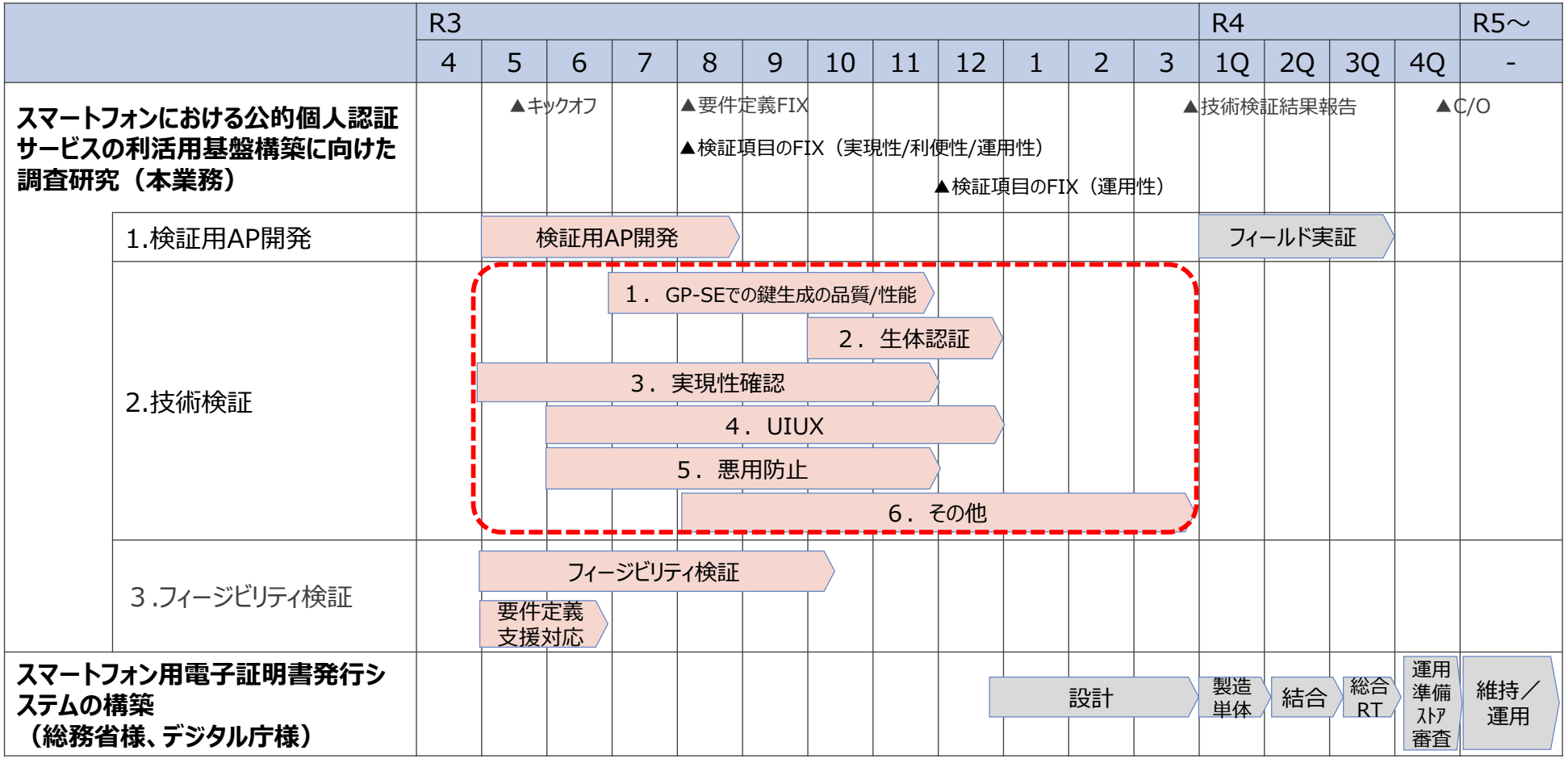
技術検証　全体概要

■ 本技術検証プロジェクトにおいては、スマホJPKIの実現に向けて現在主に下記6種別のフィージビリティ検証を行っております。

#	検証種別	検証内容
1	GP-SEの鍵生成の品質/性能、セキュリティ評価	• GP-SE内での公開鍵、秘密鍵の鍵ペア生成/署名の処理時間の計測、評価の実施。 • GP-SE内で生成する乱数及び鍵の品質について、評価・認証の取得状況の整理、評価の実施。 • GP-SE、JPKIアプレットの評価スキームについての整理の実施。
2	生体認証	• スマホJPKIシステムでスマートフォンの生体認証機能を利用登録、利用する際のフィージビリティを検証する。
3	実現性確認	• 下記点においてスマホJPKIシステムにおける技術的なフィージビリティを検証する。 – スマホJPKIシステムにおける発行等の主な業務が問題なく実行できること – JPKIスマホアプリを用いてサービス提供者がサービス提供する際の方式検討
4	UIUX	• 電子証明書をスマホ実装したものを用意し、マイナポータルへのログインや各種サービスの電子申請を想定したユーザテスト／利便性確認を行う。 • スマホJPKIのユースケースを整理し、ユーザテスト・事業者ヒアリング等の計画を策定する。
5	悪用防止	• スマホJPKIサービス利用時に悪意ある第三者からの悪用を防止するために必要な対策について検討を行う。
6	その他	• スマホJPKIサービス全体のグランドデザイン、及びそれに基づく責任分界、利用者からの利用同意取得手法の検討 • その他GP-SE、アプレット関連の細かな技術的なフィージビリティの検証

全体概要スケジュール

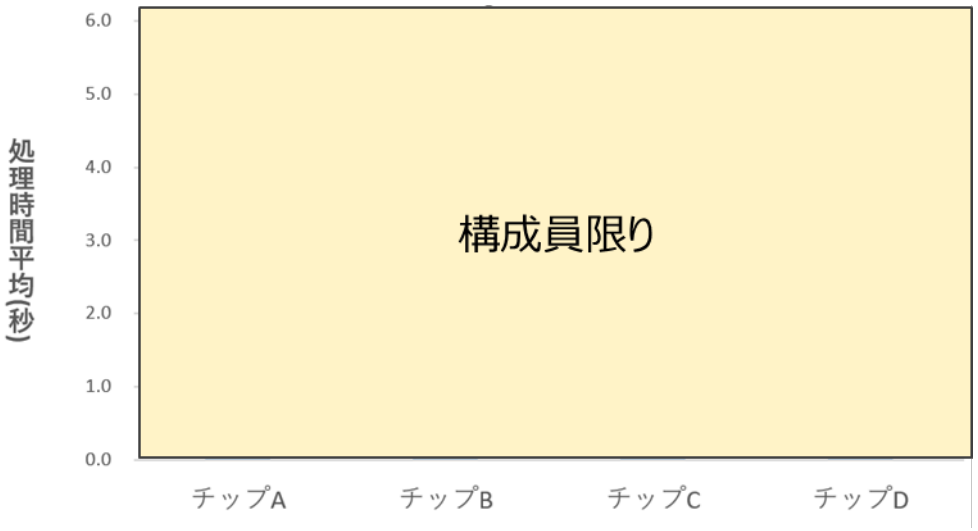
■ 前頁でお示しした検証種別について、それぞれ下記のスケジュールで進めております。（赤色点線枠）



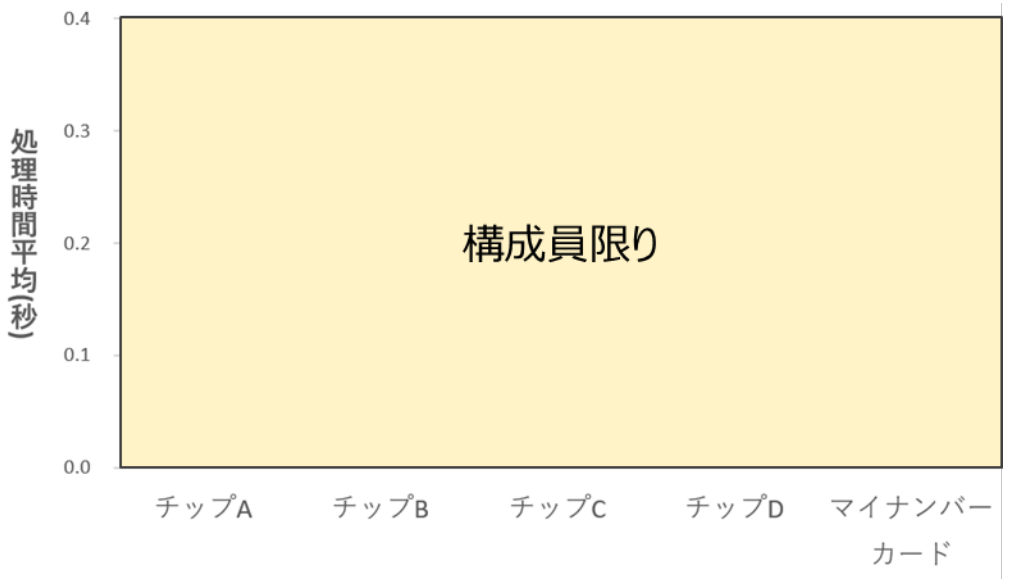
1．GP-SEの鍵生成の品質/性能、セキュリティ　（検証概要）

#	検証項目	検証項目概要	検証状況
1-1	GP-SE内での鍵ペア生成/署名処理時間	・公開鍵、秘密鍵の鍵ペア(RSA2048bit)生成の実機処理時間を計測し、評価する。 ・また、秘密鍵で署名処理を行った際の実機処理時間を計測し、評価する。	・ 鍵生成は5秒程度を想定していたが、平均2秒程度のICチップが多かった。但し、GP-SE4製品中、1製品ではばらつきが大きくUI上の検討が必要である。 ・ 署名処理はばらつきが小さい。
1-2	乱数・鍵品質確認	・GP-SE内で生成する乱数及び鍵の品質について、評価・認証の取得状況を整理し、評価を行う。	乱数：　AIS31に適合することを確認 鍵生成：FIPS PUB 186-4に適合することを確認
1-3	GP-SE、JPKIアプレット評価スキーム	・GP-SE、JPKIアプレットの安全性評価スキームの整理を行う。	・GP-SE(ICチップ、OS、JPKIアプレット)についてCC認証を取得する。販売済みスマホに搭載されたGP-SEについても認定取得可能な見込み。

【鍵ペア生成処理】



【署名処理】



1-1. GP-SEの鍵生成の品質/性能、セキュリティ（鍵生成時間のばらつき） 構成員限り

1-2. GP-SEの鍵生成の品質/性能、セキュリティ （鍵、乱数の品質）

- GP-SEが生成する鍵と乱数の品質が、HSMと同等のセキュリティレベル(EAL4+)を取得できる水準であることを確認した。
- GP-SEハードウェアが取得するCC認証の結果を参照し、第三者セキュリティ機関が確認した。
- 運用において、GP-SE新製品採用時に各規格を満たすことを確認していく必要がある。
- 最終的には、アプレットを含めてCC認証を取得することで、鍵及び乱数の品質を担保する。

＜GP-SEが満たす規格＞

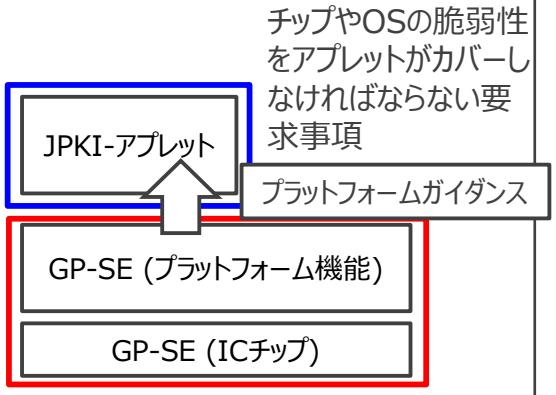
#	GP-SEチップ種別	乱数品質	鍵品質
1	チップA	AIS31	FIPS 186-4 ※1
2	チップB	AIS31	FIPS 186-4 ※1
3	チップC	AIS31	FIPS 186-4 ※1
4	チップD	AIS31	FIPS 186-4 ※1

※1 「乱数品質」列に記載の規格に基づき生成された乱数を使用して鍵を生成

・AIS31
ドイツ連邦政府の情報セキュリティ担当部門(BSI)が規定する乱数の規格。
実装すべき機能（乱数生成時に故障を検知するテストを実施する等）、統計に基づくテストと基準を規定。
・FIPS 186-4
米国標準技術研究所(NIST)が規定するデジタル署名に関する規格（鍵生成含む）。
鍵を生成するアルゴリズムを規定。

1-3． GP-SEの鍵生成の品質/性能、セキュリティ （評価スキーム）

- GP-SE内のICチップ及びプラットフォーム機能はセキュリティ評価済み（CC認証あるいはEMVCo認定）ですが、安全性の観点ではJPKIアプレット部分を含めた評価が必要と考えます。
- 以下に示す３つの評価スキームを比較検討しました結果、マイナンバーカードと同等レベルの安全性を担保するため、CC認証(下図③)を取得していきます。

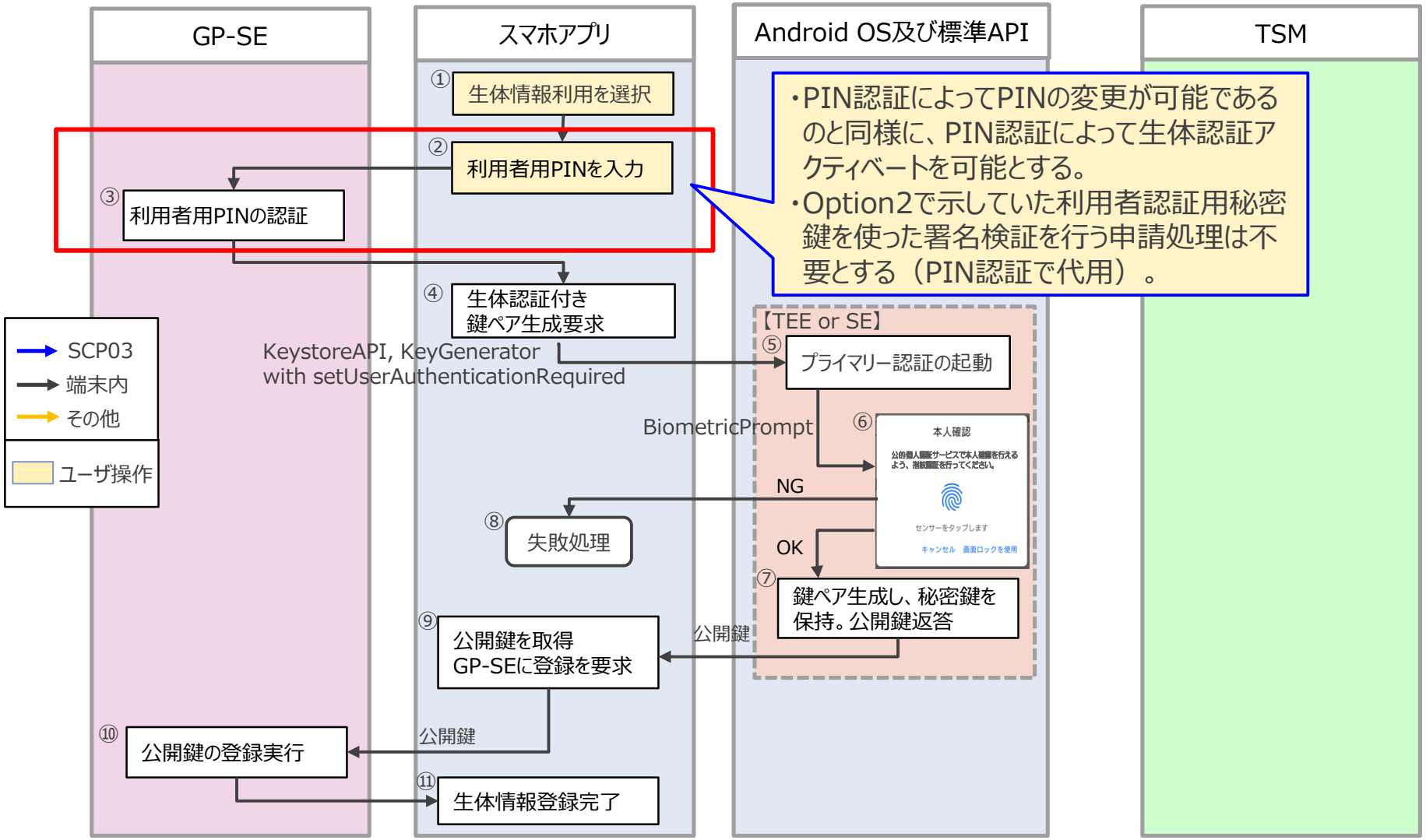
	①アプレット独自評価スキーム	②プライベート認証スキーム （脆弱性評価のみ）	③CC認証スキーム （CCによるフルスペック評価）
概要	・GP-SE (ICチップ及びプラットフォーム機能) はセキュリティ評価済み。 ・**プラットフォームガイダンス**を遵守したJPKIアプレットを開発し、ソースコードを評価機関が評価  青枠：評価対象 赤枠：セキュリティ評価済み	・GP-SE (ICチップ及びプラットフォーム機能) はセキュリティ評価済み。 ・SPをオーナーとする独自スキームを構築。 ・脆弱性評価のみを実施。  青枠：評価対象 赤枠：セキュリティ評価済み	・GP-SE はICチップあるいはプラットフォーム機能のCC認証取得済み。 ・CC認証制度に基づくスキーム構築。 ・PPに基づき、セキュリティ評価を行う。 ・GP-SEのCC認証取得状況に応じてコンポジット評価。  青枠：評価対象 赤枠：セキュリティ評価済み
評価機関	SPが指定する評価機関	SP指定する評価機関	CC認証制度に基づく評価機関
認証機関	なし	SPが指定する認証機関	CC認証制度に基づく認証機関

2．生体認証　（検証概要）

#	検証項目	検証項目概要	検証状況
2-1	生体認証アクティベート	生体認証アクティベート(利用開始)時に利用するセキュア領域にて鍵ペアが生成され、GP-SE内に鍵が保存されることを検証する。	・BiometricPromptを用いた生体認証とGP-SEの連動について実現できることを確認した。 ・第3回検討会ではアクティベートの際にTSMとの認証を行う案を示していたが、スマホ内で処理する方式とした。
2-2	生体認証利用	スマートフォンの生体認証を利用した際に生体認証の結果がGP-SEに連携され、利用者証明用証明書の認証ができることを検証する。	・登録と同様Google(US)のエンジニアによるRV実施中 ・並行して有識者より指摘のあった課題(生体認証とPIN認証を、署名検証側が識別する手段)を検討した
2-3	特定機種の利用制限	特定機種において生体認証機能に問題/不具合が発生した場合に該当機種を特定して生体認証の利用対象外にできることを検証する。	・生体認証に限らず、特定の機種に問題/不具合が発生した場合の機能として検証を実施。 ・運用に向け、脆弱性情報の申告ルート等を整備していく必要がある

2-1. 生体認証アクティベート①

- 第3回検討会で提示された生体認証アクティベートのフロー(Option1、Option2)の選定について検討しました。
- Option2の改良版として、TSMとの間の署名検証を含む申請処理を不要とし、利用者権限でアクティベートするOption2b（下図）を考案しました。Option1との比較検討の結果、Option2bを採用することします。



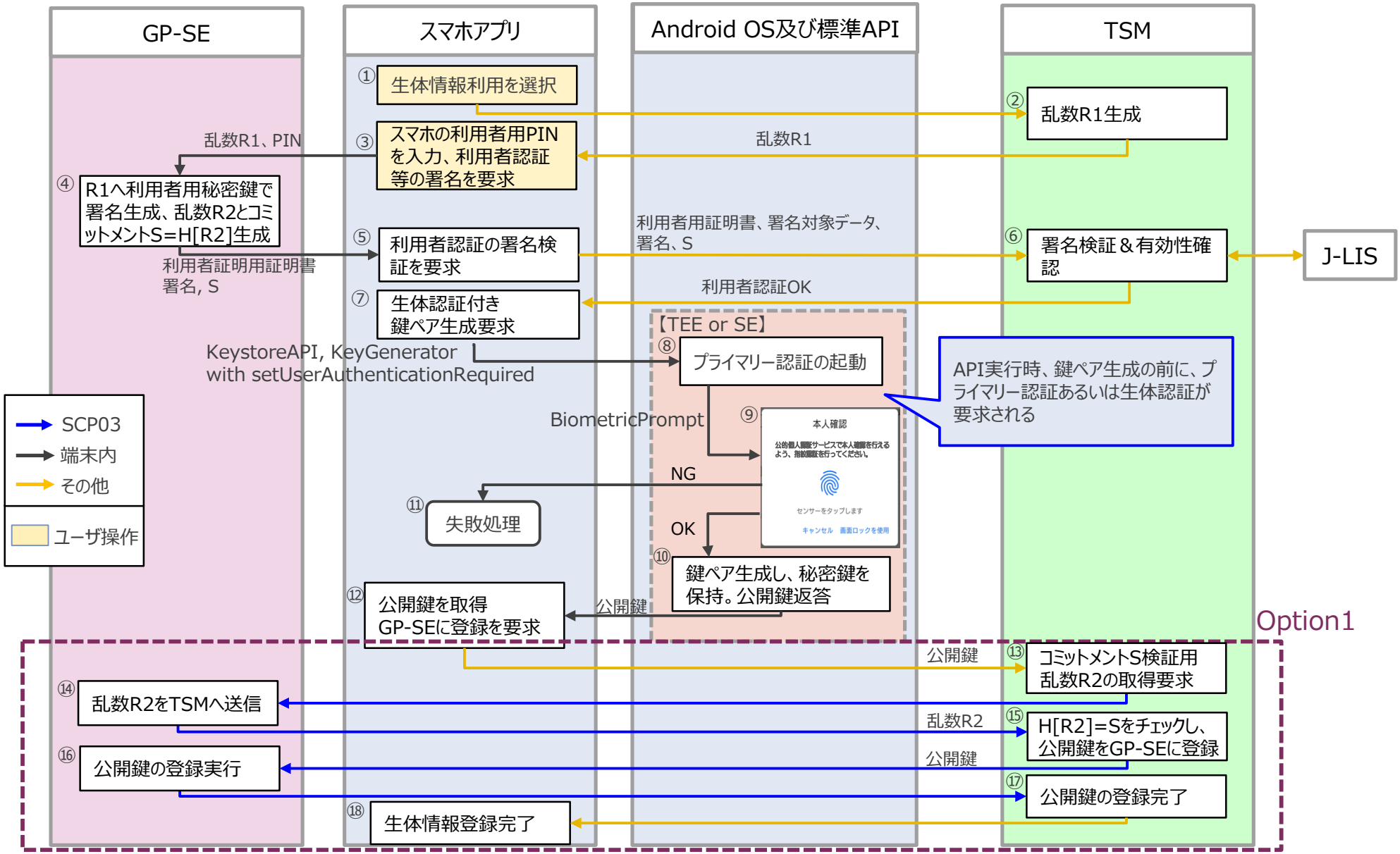
2-1. 生体認証アクティベート②

- Option1とOption2bとの比較結果を以下に示します。
- 安全性の観点では両者とも特に問題なし。フローの複雑さ、実現のためのコスト、利便性の観点からOption2bが適していると判断します。

#	項目		Option1	Option2b
1	概要		・管理者権限でアクティベートする考え方 ・申請処理有り	・利用者権限でアクティベートする考え方 ・申請処理無し
2	フローの複雑さ		△ **複雑** ・SCP必須 ・公開鍵をエクスポートする	○ **簡単** ・SCP不要 ・公開鍵をエクスポートしない
3	実現のためのコスト	開発	△ **相対的にコスト高** ・フローが複雑 ・試験工程大	○ **相対的にコスト小** ・フローが簡単 ・試験工程小
4		運用	△ **相対的にコスト高** ・申請情報の管理が発生	○ **相対的にコスト小** ・申請情報の管理不要
5	安全性		○ **特に問題なし** ・Open Mobile APIによるアクセス制御 ・SCPによる保護	○ **特に問題なし** ・Open Mobile APIによるアクセス制御 ・PINによる保護
6	利用者操作（利便性）		△ **相対的に低い** ・申請処理の煩わしさ ・処理時間がかかる （TSMとの通信が発生）	○ **相対的に高い** ・申請処理なし ・処理時間がかからない （スマホ側の処理で完結）

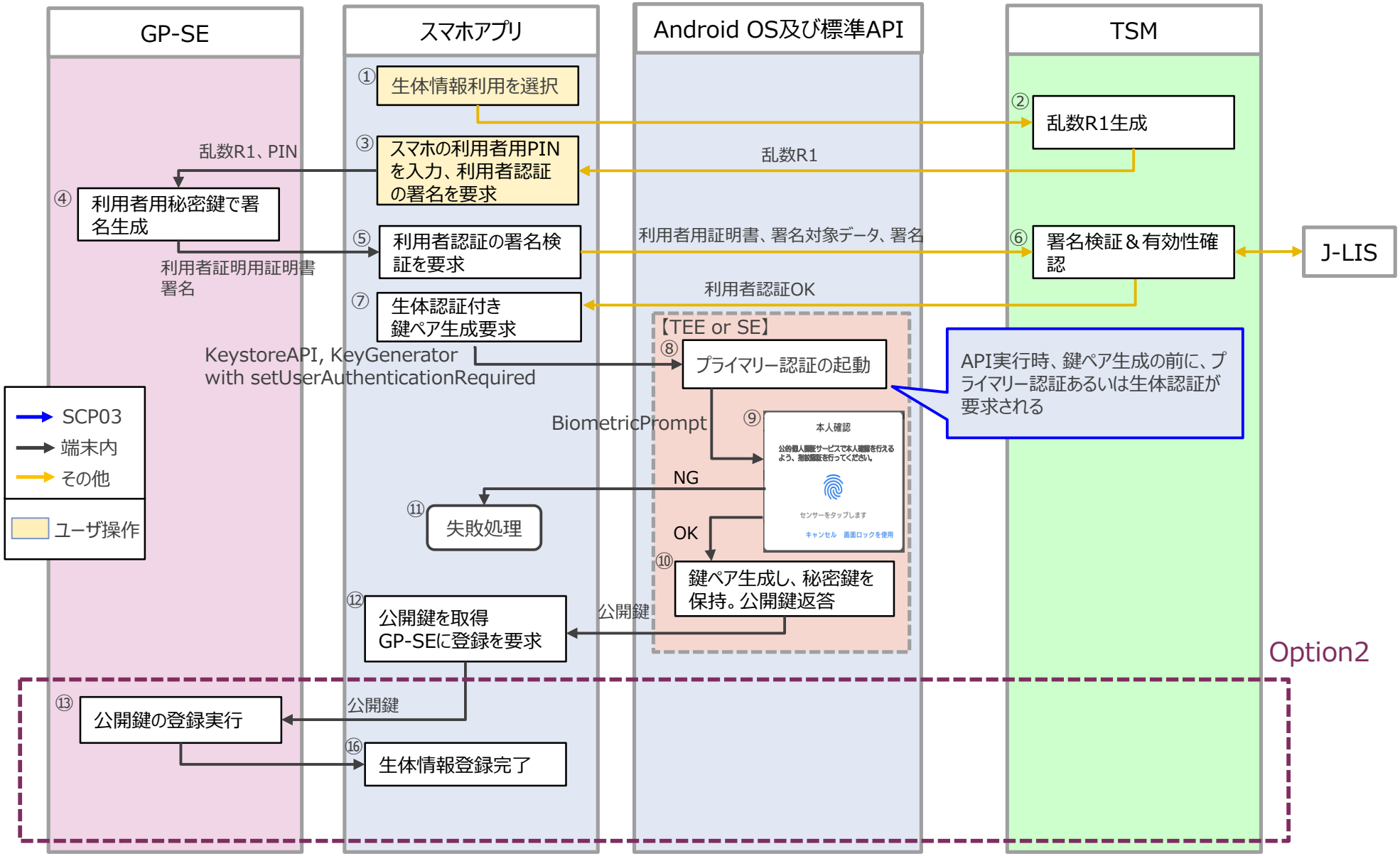
【参考】生体認証アクティベートフロー　Option1

・第3回検討会で提示されたOption1のフロー。



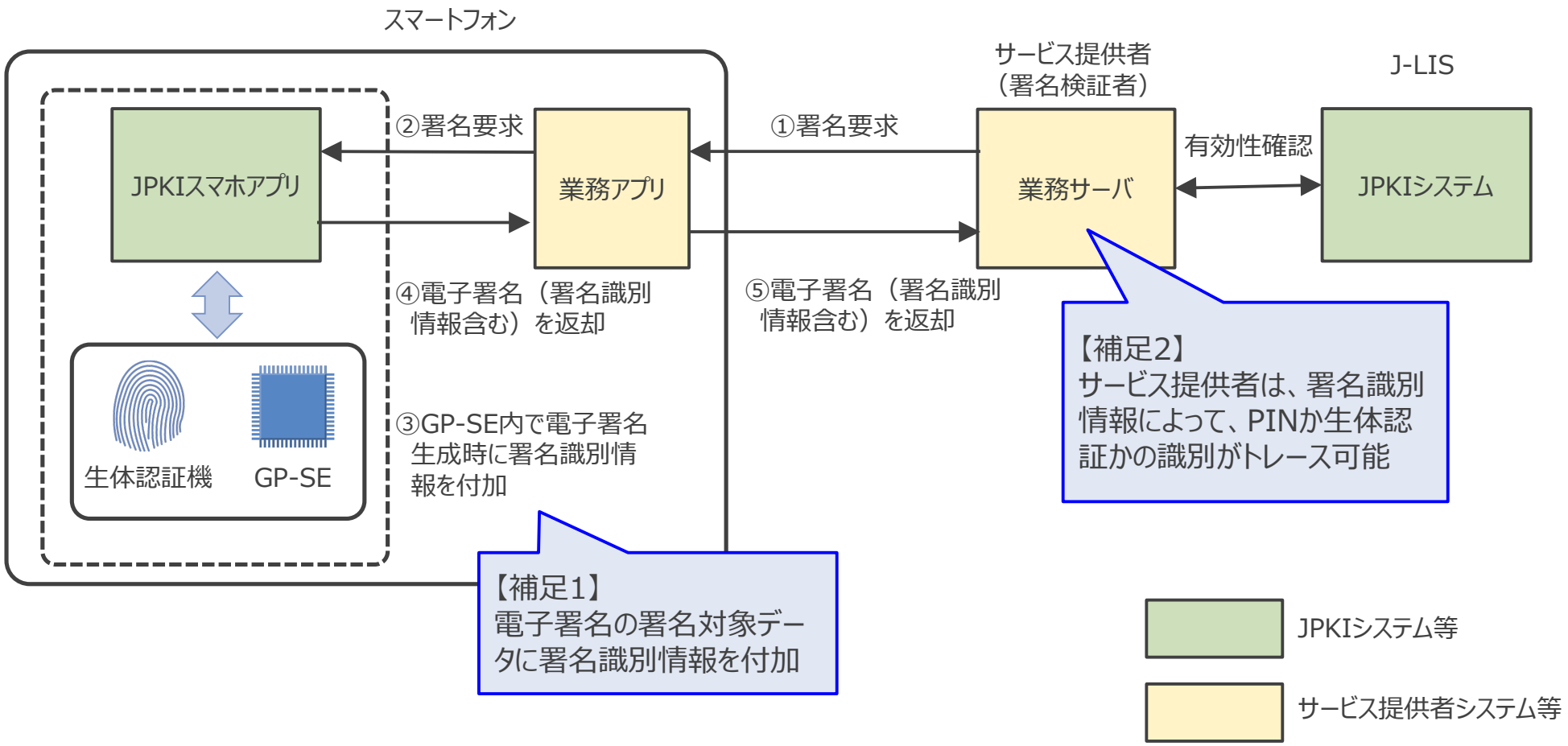
【参考】生体認証アクティベートフロー　Option2

・第3回検討会で提示されたOption2のフロー。



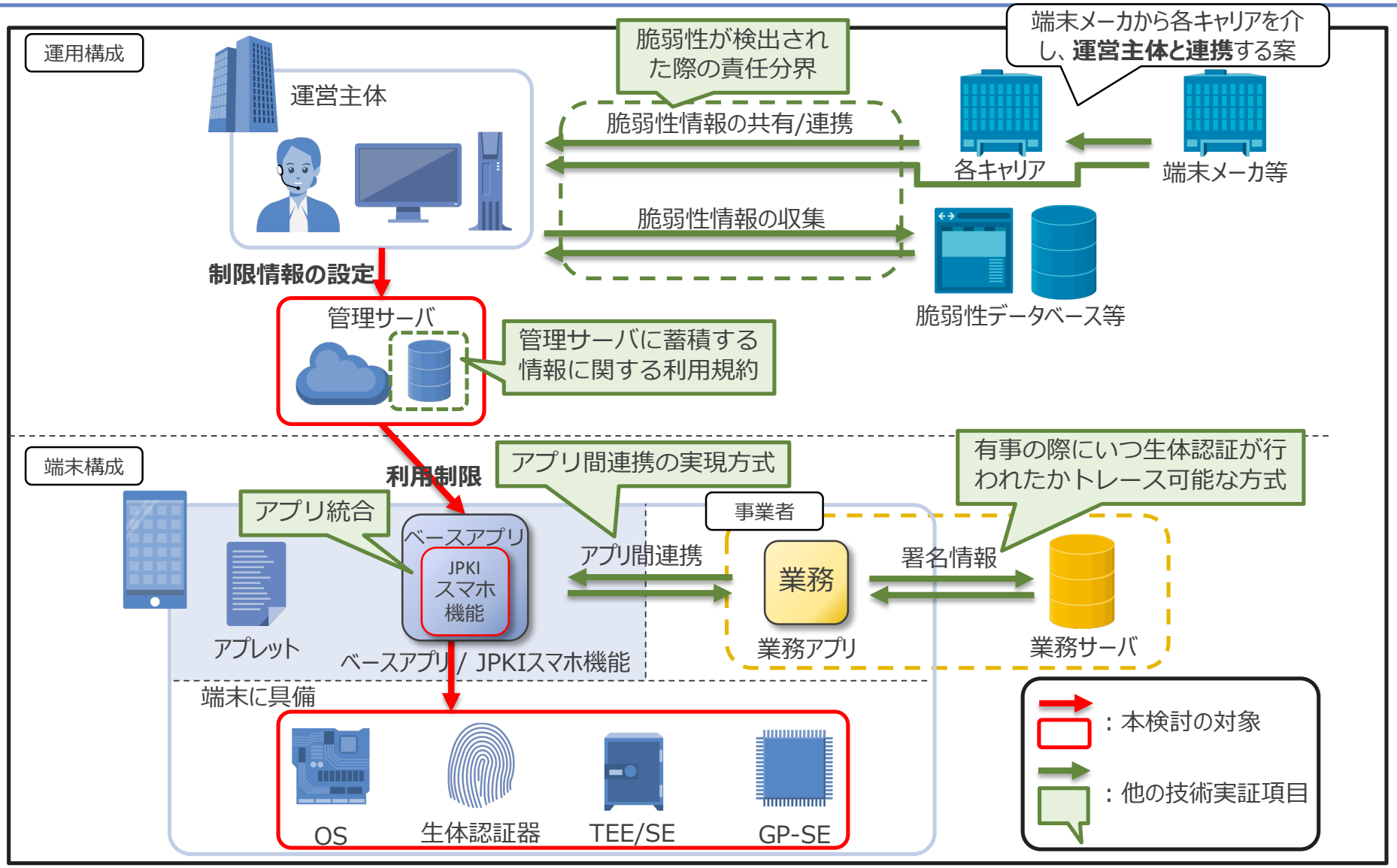
2-2．生体認証利用（PINあるいは生体認証の識別手段の提供）

- 検討会において有識者より指摘のあった課題(生体認証とPIN認証を、署名検証側が識別する手段)について検討しました。識別手段の実現方式の概要を下図に示します。
- このような識別手段によって、サービス提供者（署名検証者）はスマートフォンの生体認証等において何らかの不具合があった際にトレーサビリティを確保することが可能になります。



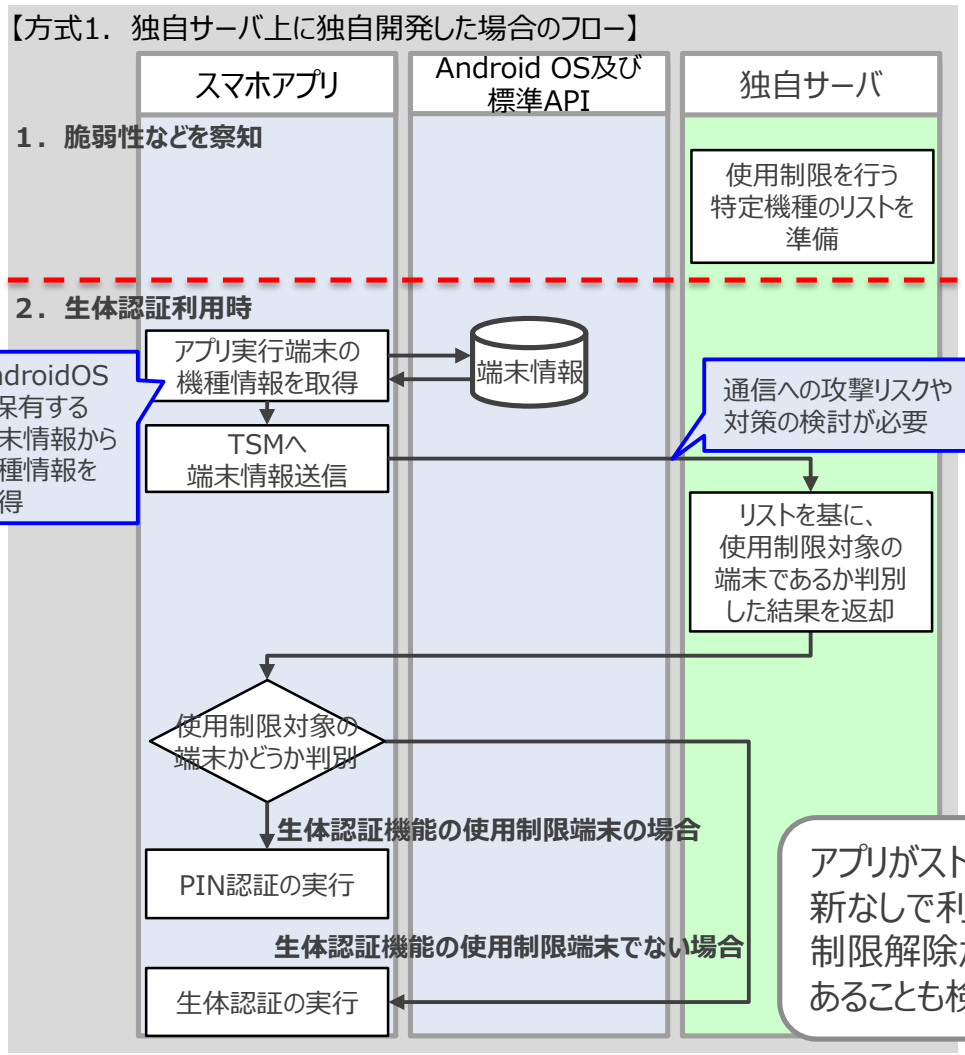
2-3．特定機種の遠隔利用制限機能：全体像

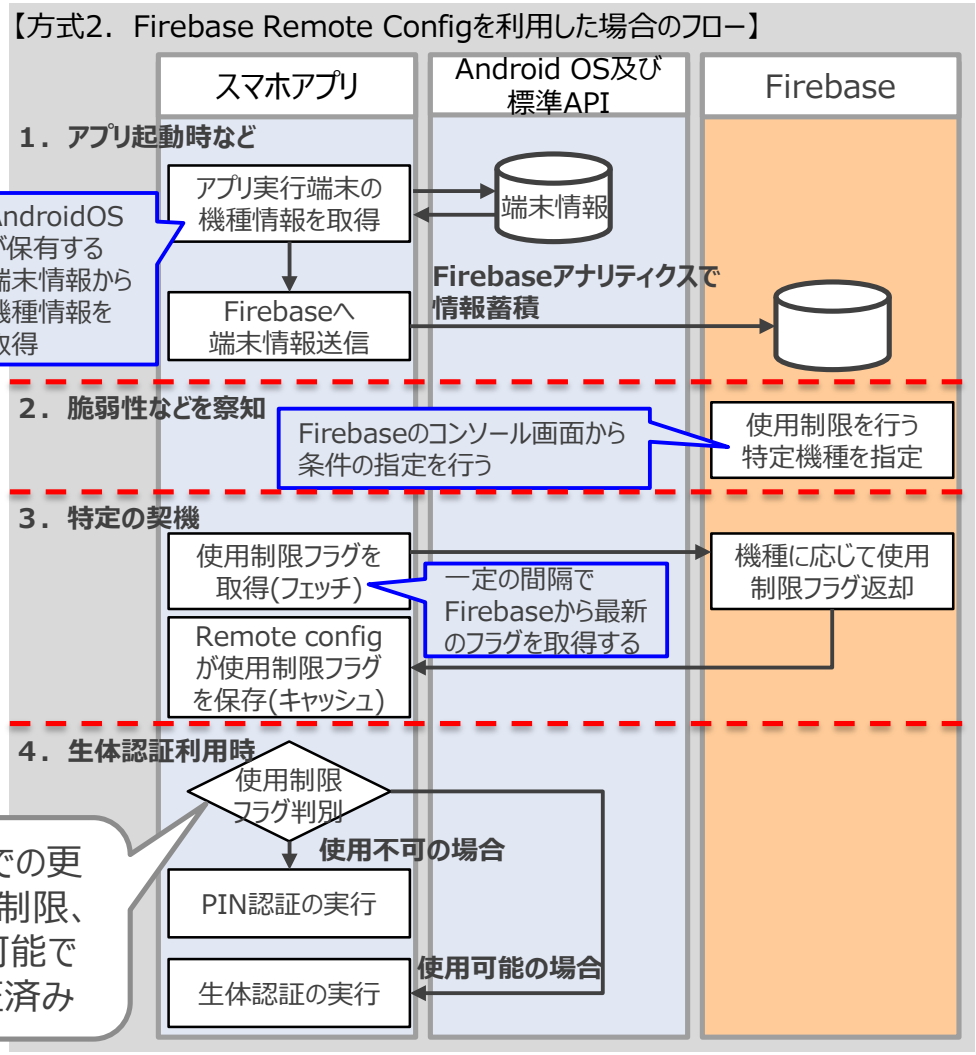
■ 特定機種の遠隔利用制限を行うための手段を検証することができたが、制限を発動することを運用上どのようにして判断するか慎重な検討が必要である。



2-3．特定機種の遠隔利用制限機能：フロー

■ Firebaseの場合はAPIを実行するだけで実現可能であるため設計・製造のコストを抑えた形で実現可能となります。ただし、即時性はなく最大で12時間程度反映に時間がかかります。





3．実現性確認　（検証概要）

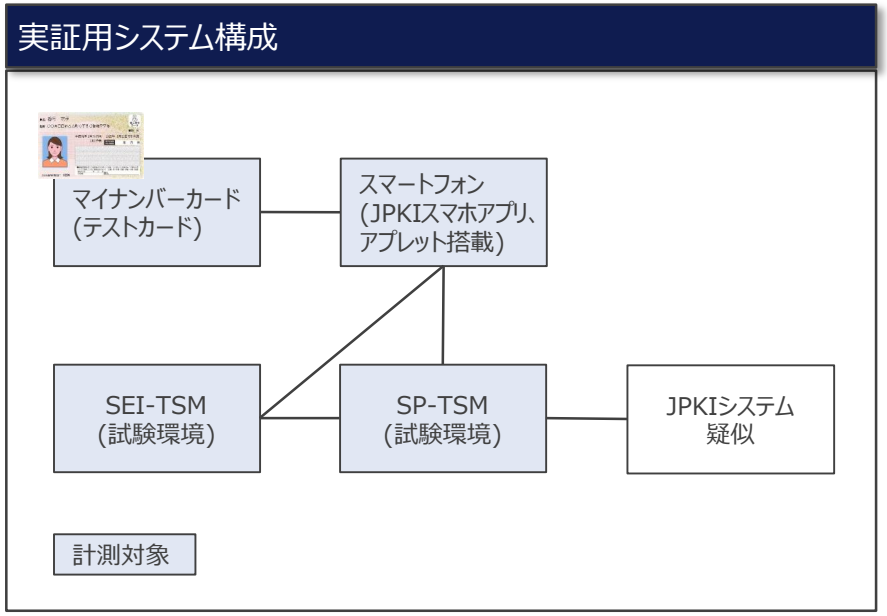
#	検証項目	検証項目概要	検証状況
3-1	フロー検証	• スマートフォン内のGP-SEにアプレットを搭載し、電子証明書発行等ができることを検証する。 • スマートフォンに搭載した電子証明書を利用するための生体認証アクティベートができることを検証する。 • オンライン利用（スマートフォンに搭載した電子証明書向けPINまたはパスワード認証による利用、生体認証による利用、画面ロック解除時の利用）が可能かを検証する。 • 各フローの処理時間を計測する	証明書発行、更新、失効等の基本的なフローが動作することを確認。スマートフォンメーカ、OSバージョンのバリエーション評価を実施し、いずれのメーカ、OSバージョンでも証明書発行、利用フローが動作することを確認。 処理時間についてはかざし利用、オンライン利用で問題ないことを確認。発行ではシステム処理におけるユーザの待ち時間を考慮した画面設計と、全体の操作時間短縮を考慮した処理の検討が必要なことを確認。
3-2	セッション中断	処理中に通信断が発生した場合に中断した処理から再開可能か継続性に関する動作検証を行う。	発行、利用等の基本フローにおいて、想定通りの箇所で通信断とから再開可能であることを確認。

3-1．フロー検証　処理時間計測（計測条件）

■ スマートフォンと検証用TSMを用いて、各業務フローの全体時間測定と区間測定を行い、想定されるユーザ待ち合わせ時間の算出や機種毎の処理時間の差を計測し、本開発に向けた性能課題抽出と対応方針を検討した

[計測条件]
・右記の対象機種に対し、各機種10回計測し、平均時間、最大時間、最小時間を取得する。
・JPKIシステムは、疑似装置で計測する。(計測対象外とする)

[計測環境]



[計測機種]
・メーカ、SoC、GP-SE種別、発売年度、OSバージョン、クラスのバリエーションを考慮した以下の機種で計測する。

#	端末	SoC	GP-SE種別	発売年度	OS Ver	クラス
1	端末A	構成員限り				
2	端末B					
3	端末C					
4	端末D					
5	端末E					
6	端末F					
7	端末G					
8	端末H					
9	端末I					
10	端末J					

3-1．フロー検証　処理時間計測（結果まとめ）

■ ターンアラウンドタイムを計測した結果、発行においてユーザの待ち時間を考慮した画面、処理設計を行う必要があることを確認した

#	項目	結果	考察
1	発行	・発行フローは短くても90秒程度である。 ・ユーザ待ち合わせは25秒程度である。	・ユーザの待ち時間を考慮した画面設計と、処理のパラレル化を採用する必要がある。 ⇒署名用パスワード設定と利用者証明用PIN設定におけるユーザ操作 (23秒程度)と処理の並列化を行っていく
		・機種によりOpen Mobile API処理時間に差がある。 ・機種により鍵ペア生成時間に差がある。 (検証項目「GP-SE内での鍵ペア生成・署名処理時間」と同結果)	・Open Mobile APIの処理時間の差は、特定機種のみのため、要因を端末メーカーに確認する。 ・本開発においても、対象全機種のターンアラウンド計測を行うことが望ましい。
2	かざし利用	・かざし利用は、1秒程度である。	・かざし利用における待ち時間は、ユーザが感じないと考えられる。
3	オンライン利用 (生体認証)	・オンライン利用は、8秒程度である。 ・機種によりOpen Mobile API処理時間に差がある。(＃1発行と同結果)	・オンライン利用における待ち時間は、ユーザが感じないと考えられる。

参考．3-1フロー検証補足資料：測定結果（発行）

■ 署名用と利用者証明用の同時発行時のターンアラウンドタイムを計測した結果は次の通り
・一連の発行フロー(PIN/パスワード初期設定含む)全体は、90秒程度であった。
ただし、不慣れなユーザの場合＋30~60秒程度の追加が見込まれる。
・ユーザ待ち合わせ時間(鍵ペア生成~電子証明書格納)は、24秒程度であった。
ただし、鍵ペア生成時間のバラつきを考慮すると、20~40秒程度が見込まれる。
■ 機種毎の処理時間にバラつきが有り、以下の傾向について分析を実施している
・端末Fのアプレットの処理時間が長い。
・端末Hの鍵ペア生成時間が長い。

【発行フローのターンアラウンドタイム計測結果(全機種平均値)】

計測区間	計測時間(秒)	(内訳)					
		ユーザ操作時間(秒)	各システム処理時間(秒)				
			スマホアプリ	(対アプリ)アプレット	(対TSM)アプレット	TSM	JPKIシステム(想定)
① 発行申請	18.1	14.6	2.1	0.3	0.1	0.0	1.0
② 署名用パスワード設定	16.0	13.1	–	0.7	1.6	0.7	–
③ 利用者証明用PIN設定	13.2	10.3	–	0.6	1.6	0.7	–
④ 署名用鍵ペア生成	4.6	–		–	3.9	0.7	–
⑤ 署名用電子証明書格納	7.4				1.9	0.5	5.0
⑥ 利用者証明用鍵ペア生成	3.3			–	2.8	0.5	–
⑦ 利用者証明用電子証明書格納	8.2	–	–	–	2.3	0.9	5.0
⑧ 署名用電子証明書動作検証	12.2	10.9	0.0	1.2	–	–	–
⑨ 利用者証明用電子証明書動作検証	8.0	6.8	0.0	1.2	–		
合計	91.0	55.7	2.1	4.0	14.2	3.9	11.0

合わせて24秒

【機種毎の計測結果(平均値)】

構成員限り

参考．3-1フロー検証補足資料：測定結果（かざし利用、オンライン利用）

■ かざし利用時のターンアラウンドタイムを計測した結果は次の通りです。
・かざし利用における署名生成は、1秒程度の見込みである。
・機種毎のバラつきは小さい。

■ オンライン利用(生体認証)時のターンアラウンドタイムを計測した結果は次の通りです。
・ユーザ操作時間(5秒程度)を加えて8秒程度であり、マイナンバーカード利用時よりも短縮される見込みである。
・発行時と同様、アプレット処理時間が長い機種が存在する。

【かざし利用の機種毎の計測結果(平均値)】

構成員限り

【オンライン利用の機種毎の計測結果(平均値)】

構成員限り

４．UI／UX

#	検証項目	検証項目概要	検証状況
4-1	アプリ一体化	複数の行政アプリが出現することを考慮し、機能の切り分けや提供方法などについて柔軟に対応可能なつくりとするための方式について検討する。	統合対象のアプリについて、メリット・デメリットを精査し、統合方式や統合可否について検討中。併せてマイナポータルアプリへの統合を仮定し統合方針を具体化中。
4-2	Firebase等解析ツールの活用	Firebase等解析ツールの活用等による画面遷移や操作ログの分析手法について検討し、設計工程に向けた提言を行う。	取得ログ情報や分析頻度、クラッシュ情報等の活用に向けた検討を実施中
4-3	署名の重要性を認識しやすい設計	署名用証明書の重要性を認識しやすい仕組みについて検討し、設計工程に向けた提言を行う。	画面上への表示の仕組み等、認識しやすい方法・方式を検討中
4-4	模擬マイナポータルログイン	電子証明書をスマホ実装したものを用意し、マイナポータルへのログインや各種サービスの電子申請を想定した利便性確認を行う。	10月下旬～11月中旬にかけてユーザテストを実施。ユーザテスト結果について分析・取りまとめを行い、設計工程に向けたインプットを作成した。
4-5	スマホJPKI利用ユースケースの実証検討	スマホJPKIのユースケースを整理し、ユーザテスト・事業者ヒアリング等の計画を策定する。	関連する事業者・関連部署に対し、依頼／確認事項を整理し、ご説明・ご協力依頼を実施予定

4-4．UI／UX（模擬マイナポータルログイン（ユーザテスト実施概要））

■目的
マイナポータルアプリにおける基本機能（発行申請、生体認証登録、マイナポータルログイン、機種変更）をユーザがスムーズに利用できるかどうか検証すること

■評価観点
本ユーザテストにて、本アプリのユーザ操作の記録・観察、及び操作後のインタビューを実施し、以下の2つの観点を評価します。

1：既存の利用方法からのUX向上度合い
- 既存の利用方法よりも便利になっていること
- これまでと変わらず、安心安全に使用できること

2：本アプリでの新しい利用方法によるユーザビリティ品質(※)
1.ユーザが**目標を達成**できること
-シナリオを達成できるかをテストし、運用の実現性を評価。
2.ユーザが**効率的**に目標を達成できること
-期待と異なる画面遷移、不要な操作ステップがないかをテストし、作業効率性を評価
3.ユーザが**満足**しているか
-改悪されていないか、改善点がないかをテストし、ユーザ満足度を評価

※ユーザビリティ品質の3つの観点はISOで規定されているユーザビリティの定義より引用：ISO 9241-11/JIS Z 8521

４-４．UI／UX（模擬マイナポータルログイン（テスト対象者））

以下の3つのセグメント（各セグメント10名ずつ）に対しテストを実施

① ITリテラシが高い若・中年層
② ITリテラシが低い若・中年層
③ ITリテラシを有する高齢層

＜参考＞
■年齢層
・若・中年層：20～59歳
・高齢層：60歳以上

■ITリテラシ（被験者募集要件）
被験者をリクルートするための条件として、以下の4項目をITリテラシーの有無の判断基準として設定
(1)スマホで何らかの申込をしたことがある
(2)スマホで生体認証を利用している
(3)NFCを利用している
(4)Wi-Fi、Bluetoothの設定ができる

ITリテラシが高い⇒**4つすべて**に該当
ITリテラシが低い⇒該当する項目が**2つ以下**
ITリテラシを有する⇒該当する項目が**1つ以上**

4-4．UI／UX（模擬マイナポータルログイン（ユーザテストの流れ））

No.	シナリオ分類	バリエーション	検証目的
1	発行申請	**①発行申請**	新規利用手続きをスムーズに行えるか、躓かないか確認（利用を諦めることにならないか確認）
2	機種変更	**②機種変更手順１** 新端末からの発行申請	機種変更に係る操作を問題なく実施できるか確認
		③機種変更手順２ 旧端末での失効＋新端末からの発行申請	
3	生体認証利用登録	**④生体認証利用登録手順１** 端末に生体認証をすでに設定している場合	・(特に高齢者等が)生体認証利用登録を問題なく実施できるか確認 ・生体認証に抵抗は無いか確認
		⑤生体認証利用登録手順２ 端末に生体認証が未登録の場合、登録から実施	
4	マイナポータルログイン	**⑥新ログイン方法１（生体認証）**	・生体認証等、各種認証を使用して問題なくログインできるかを確認 ・生体認証を使用することで、PINやパターン認証より使い勝手が良くなるかを確認
		⑦新ログイン方法２（パターン認証）	
		⑧新ログイン方法３（PIN認証）	
		⑨新ログイン方法４ **（生体認証→PIN/パターン認証に切り替え）**	
		⑩マイナポータルへの既存ログイン方法	マイナンバーカードをスマホに搭載することで、使い勝手が良くなるかを確認

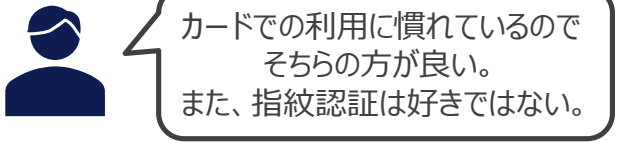
４-４．UI／UX（模擬マイナポータルログイン（結果総評／サマリ））

1．既存の利用方法からのUX向上度合い

✓ 既存の利用方法よりも**便利**になっていること

⇒マイナンバーカード機能をスマホに登録することで、スマホ単体でマイナポータルのコンテンツを閲覧できることについては30人中29人が好感を持っていた。

＜既存の利用方法を好む人＞



✓ これまでと変わらず、**安心安全**に使用できること

⇒生体認証やパターン認証によるログインは、マイナンバーカードをかざしてログインをする既存の方法と比較すると、PIN／パスワード忘れや漏洩の防止に繋がり、安心安全に利用できると、被験者から好まれる様子が見られた。

2. 本アプリでの新しい利用方法によるユーザビリティ品質（総評）

✓ 総評

⇒個々の機能の操作ではユーザの躓きや迷いは少なかったため、満足度も高くユーザビリティ品質は良好であると判断する。しかしながら、現行マイナポータルの画面を大きく変えずに、JPKIの導線を追加する形でプロトタイプを作成したため、JPKIアプリに行きつくための導線が発見しにくいUIとなり、トータルでの目標の達成率や達成時間に影響を及ぼした。テストにより現行マイナポータルを考慮した総合的な導線設計の示唆が得られた。

2. 本アプリでの新しい利用方法によるユーザビリティ品質（個別観点）

✓ ユーザが**目標を達成**できること

⇒現行マイナポータルアプリからJPKIスマホアプリまでの導線の入り口がわかりづらく、モデレータの助言が必要となるユーザも多く、自力での目標達成が難しい様子が見られたが、 JPKIスマホアプリの導線に入ってしまえば、その後は比較的スムーズに操作できている様子が見られた。

✓ ユーザが**効率的**に目標を達成できること

⇒現行マイナポータルアプリからJPKIスマホアプリまでの導線の入り口がわかりづらく、ユーザが各タスクの目的を達成するための画面がどこにあるか探せず、ステップ数や時間に大きく影響を及ぼした。ただし、JPKIスマホアプリの導線に入ってしまえば、その後は比較的スムーズに操作できている様子が見られた。

✓ ユーザが**満足**していること

⇒生体認証登録や機種変更時の手続きにおいて、説明の長さや内容、導線のわかりづらさでユーザの満足度が下がる場面もあったが、マイナンバーカードをかざす代わりに生体認証等のスマホの認証機能でアプリを利用できることは、満足度の高い傾向が見られた。

4-4．UI／UX（模擬マイナポータルログイン（結果総評／サマリ：シナリオ））

ユーザテストの実施シナリオごとに今後の画面設計における重要な気づきが得ることが出来た。
※今回使用したプロトタイプでは、既存のマイナポータールありきで検討したため、スムーズな導線設計ができなかった。
以下のサマリには、その影響による結果は除外したものを記載。

シナリオ		発行申請	生体認証登録	マイナポータル ログイン	機種変更
テスト結果	リテラシ高	✓ 一度手続きの流れに乗ってしまえば、その後は比較的スムーズに操作できている様子が見られた	✓ 途中でOSの設定画面に遷移したこと、指紋登録後にマイナポータルに戻る必要があることを理解できていた。	✓ 問題なくログインし、利用できる。 ✓ 普段生体認証を使っていないユーザでも、スムーズに生体認証を使用することができる。	✓ どこから手続きをするのかわからず、困っている様子が見られた。
	リテラシ低	✓ マイナンバーカード読み取りの際、スマホのカメラでカードを読み取るものだと誤認することで、マイナンバーカードとスマホを密着させずに読み取りを行おうとするユーザが一定数存在した。	✓ 生体認証の設定画面の説明をほとんど読まず、いきなりOSの設定画面に遷移したことに驚く様子が見られた。 ✓ OSの設定画面に遷移していることに気付かない。		
	高齢者				
		× マイナンバーカード読み取り方法を理解させる工夫が必要	× スマホに生体認証未設定時の導線に考慮が必要	○ スムーズな操作が可能。	× 機種変更手続きの導線に考慮が必要

4-4．UI／UX（模擬マイナポータルログイン（結果：発行申請シナリオ））

課題

事象	**アプリメニューに気付かない。**
考察	メニューが2つ存在するUIにユーザが慣れておらず、右上のメニューにのみ注目してしまうため。

発生人数	①：6/10人
	②：9/10人
	③：7/10人

改善方針	**アプリの設定・管理機能の所在がどこにあるか明瞭に分かるようにする。**

4-5．UI／UX（スマホJPKI利用ユースケースの実証検討）

- 事業者ヒアリングの検証点、検証手法は下記の通りとなります。

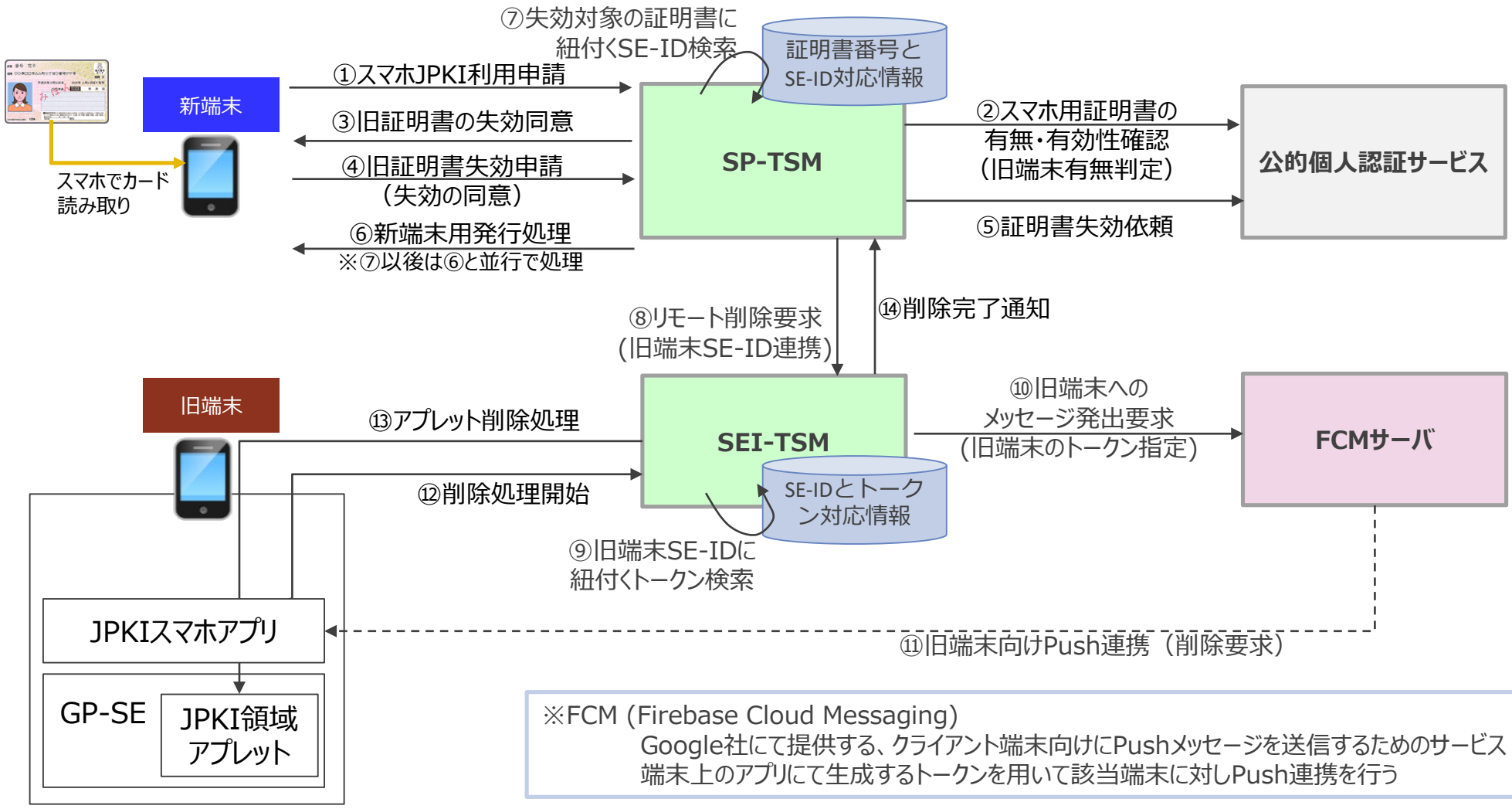
調査目的	**事業者側の視点で見たとき、現在のサービスに対して「公的個人認証スマホアプリ」を導入した際の事業者業務・ユーザ体験の懸念点・メリットを明らかにする**
検証点	**A) 価値向上：**事業者側が提供するサービスの付加価値、ユーザ体験を向上できるか **B) 快適性向上：**事業者側として、ユーザが現在より快適かつ手軽にサービスを利用できるようになると思うか **C) 利便性向上：**事業者側の業務上、不便になる点・懸念は無いか、便利になる点・期待はあるか
手法	**サービス関連事業者に対するインタビュー** • ぴったり連携サービス：インタビュー先を調整中 • 健康保険証利用：インタビュー先を調整中 • 銀行口座開設：インタビュー先を調整中
インタビュー内容例	【事業者目線に立った確認】 1．サービス想定を説明した上での事業者側業務の変化についてヒアリング 2．業務変化による懸念点・業務改善はあるかのヒアリング 【利用者目線に立った確認】 3．ユーザ側に想定される体験変化についてヒアリング 4．体験変化において、懸念点・体験向上はあるかのヒアリング 5．その他、要望等のヒアリング

5．悪用防止　（検証概要）

#	検証項目	検証項目概要	検証状況
5-1	鍵、証明書削除	悪用防止のために旧端末に存在する鍵、証明書が削除可能かどうかを検証する	旧端末がユーザの手元になく、オフラインの場合は鍵、証明書を消せないことを確認。但し、外から読み出すことはできず、当該端末の次の利用者がスマホJPKIを利用するために発行すると消去（上書き）され、事実上悪用ができないことを確認。
5-2	リモート失効・削除	GP-SEに残留したJPKIアプレットと失効済の電子証明書等について本人操作ではなくリモートで削除可能かを検証する。	Push通知を用いることで旧端末内のJPKIアプレットを削除することが可能なことを確認できた。
5-3	SafetyNet Attestation APIの活用	不正な端末における操作を防止するため、root化した端末をSafetyNet Attestation APIを用いて検知可能かどうか検証する。	デバイスの完全性パラメータであるctsProfileMatch, basicIntegrityに加え、Key Attestationに基づくevaluationTypeを用いることでroot化、root化隠蔽、カスタムROMなどを検知できることを確認できた。

5-2．悪用防止　（リモート削除）

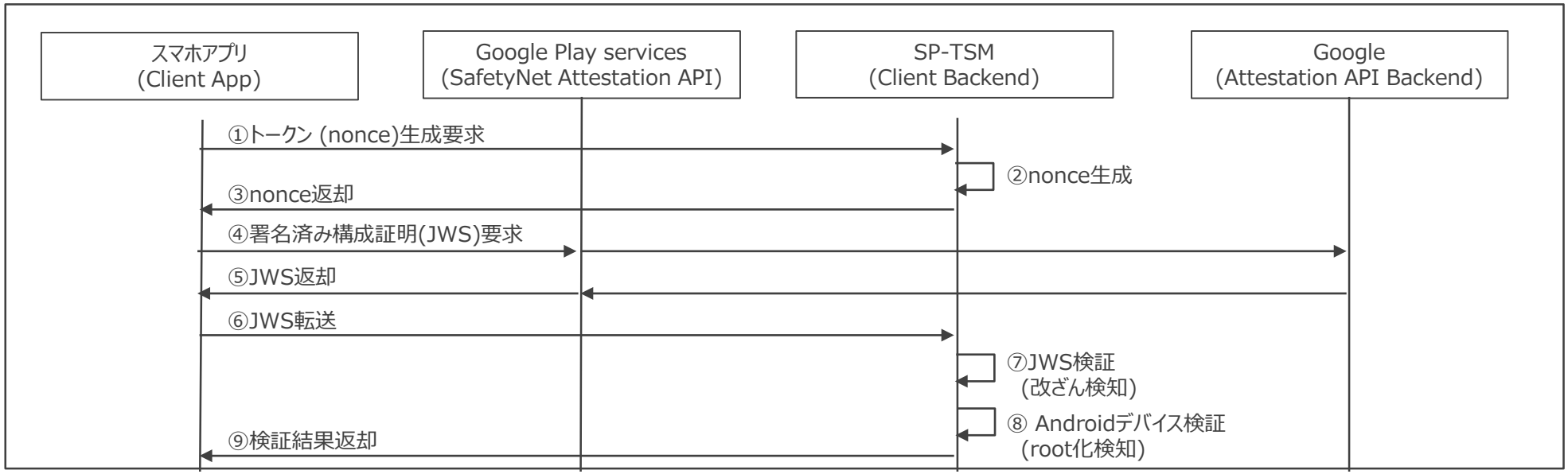
旧端末でスマホ用電子証明書の失効手続きを行わず、新端末でスマホ用電子証明書の新規利用手続きを行った場合、FCM(※)サーバによるPush連携を利用し旧端末のリモート削除処理が行われる



※FCM (Firebase Cloud Messaging)
Google社にて提供する、クライアント端末向けにPushメッセージを送信するためのサービス
端末上のアプリにて生成するトークンを用いて該当端末に対しPush連携を行う

5-3．悪用防止　（SafetyNet Attestation API　概要）

■ 端末の構成証明をSafetyNet Attestation APIを利用して端末の構成情報をGoogleのバックエンドサーバに送信し、検証結果を受信することで端末の状態を確認することができます。



#	代表的な構成情報	内容
1	ctsProfileMatch (デバイスの完全性 – strict)	デバイスの完全性に関する厳密な判定結果。Googleの互換性認証を受けており、改変されていない端末の場合にだけtrueになる。下記のような端末ではfalseとなる。 ・ブートローダーがアンロックされている端末 ・カスタムシステムイメージ(カスタムROM)が搭載されている端末 ・メーカーがGoogleの互換性認証を申請していない、あるいはそれに合格していない端末
2	basicIntegrity (デバイスの完全性 - lenient)	デバイスの完全性に関する緩やかな判定結果。 root化端末、エミュレータ、仮想端末、APIフックなどの改ざんが検知された端末ではfalseとなる。
3	evaluationType	評価結果の測定方法。BASICとHARDWARE_BACKEDがあり、後者はKey Attestation(鍵構成証明)を利用するため、Android8.0以降で利用可能。

5-3．悪用防止　（SafetyNet Attestation API／抜粋）

投影のみ
（配布対象外）

6．その他検証項目　（検証概要）

#	検証項目	検証項目概要	検証状況
6-1	アプリの利用同意	スマートフォン向けアプリの利用規約や利用者からの同意取得の方法を検討する。	マイナポータル、dアカウント、交通系サービス等の利用規約および責任分界の検討結果から、ユーザへの同意内容を整理中
6-2	責任分界検討	スマートフォン向けアプリの利用者、スマートフォン端末メーカー及び連携先であるJ-LISの責任分界を検討する。	キャリア、メーカ等へのヒアリングを行い、スマホのエコシステムを参考に責任分界を整理中
6-3	GP-SE上の他サービスアプリケーションとの共存による相互影響有無	GP-SE上に他サービスのアプリケーションがインストールされ利用される場合の、JPKIアプレットとの相互影響有無について、運用上の課題の抽出、対応事項の整理を行う。	JPKIアプレットと他サービス用アプレットへ同時アクセス時にエラーが発生する場合があるが、設計時に考慮することで回避可能である。また、GP-SE容量不足時の挙動を設計する必要がある。
6-4	アプレットサイズ	アプレットサイズの上限が64KBであるため、サイズ内に収める実装が可能か検証を行う。アプレットサイズが64kbを超える場合はその対策を検討する。	検証において作成したアプレットは30KB未満であり、異常系処理・セキュアコーディングを加味しても45KB程度となる見込み。
6-5	アクセス元の識別	GP-SEに対するアクセス元が外部のICカードリーダとスマートフォン内アプリの何れであるか識別できることを検証する。	全種類のGP-SEで問題なく識別可能なことを確認。但し、本機能はICチップに依存した機能であるため、活用していく場合は新チップ投入毎に動作検証が必要。
6-6	かざし利用の通信性能	かざし利用を想定し、マイナンバーカード対応のICカードリーダとスマートフォンが正常に通信できるかを検証する。	特定の組合せでエラーが発生したが、ICカードリーダのファームウェアアップデートにより、解消となる見込み。ICカードリーダがTypeA/B両方をサポートする場合、TypeAで通信する可能性があると判明。

かざし利用の通信性能

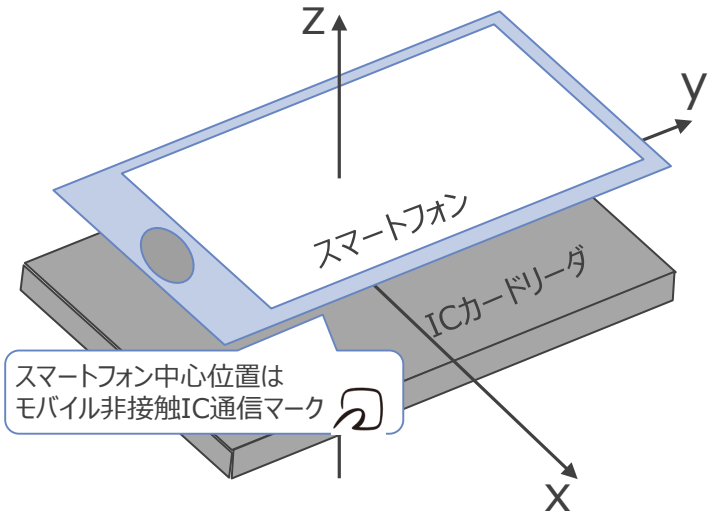
- 特定のICカードリーダとスマートフォンの組合せで通信エラーが発生したがICカードリーダのファームウェア更新で解消見込み。
- ICカードリーダがTypeA/B両方サポートする場合、TypeAで通信してしまう可能性があるという課題が判明。
- スマートフォン、ICカードリーダの双方に基準を策定し、かざし利用が実現できるよう推進する。

スマートフォン	ICカードリーダA		ICカードリーダB		ICカードリーダC	
機種	Z=0mm	Z=10mm	Z=0mm	Z=10mm	Z=0mm	Z=10mm
マイナンバーカード	●	●	●	●	●	●
スマートフォン1	●	●	●	●●●	●	●
スマートフォン2	●	●	●	●●	●	●
スマートフォン3	●	●	●	●●●	●	●
スマートフォン4	●●	●	●	●	●	●
スマートフォン5	●	●●	●●	●●●	●●●	●●●

●1回目の試行で成功
●1回目の試行で失敗、2回目で成功
●1回目2回目の試行で失敗

ICカードリーダに原因があり、ICカードリーダのファームウェア更新で解消見込み

X,Y,Z軸方向に10mmずらした位置にスマートフォンを設置し、通信可否を確認した。



【スマートフォンの設置位置の定義】